nally stored therein based upon the received update information.

[0032] According to this construction, the analyzing condition can be changed by an instruction from the content management center that manages content.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033] These and other objects, advantages and features of the invention will become apparent from the following description thereof taken in conjunction with the accompanying drawings that illustrate a specific embodiment of the invention. In the drawings:

FIG. 1 shows the construction of a content-log analyzing system 1;
FIG. 2 is a block diagram showing the construction of a broadcast receiving device 10;
FIG. 3 shows the data structure of encrypted content;
FIG. 4 is a block diagram showing the construction of a TV 20;
FIG. 5 is a block diagram showing the construction of a PC 30;
FIG. 6 is a block diagram showing the construction of a data-communication controlling device 40;
FIG. 7A shows key information stored in a decrypting unit 404 of the data-communication controlling device 40;
FIG. 7B shows key information stored in an encrypting unit 405 of the data-communication controlling device 40;
FIG. 8 shows the data structure of an address conversion table stored in the data-communication controlling device 40;
FIG. 9 shows the data structure of a content-log table stored in the data-communication controlling device 40;
FIG. 10 is a block diagram showing the construction of a content-log analyzing server 50;
FIG. 11 is a flowchart showing the operation of the content-log analyzing system 1, to be continued to FIG. 12;
FIG. 12 is a flowchart showing the operation of the content-log analyzing system 1, to be continued to FIG. 13;
FIG. 13 is a flowchart showing the operation of the content-log analyzing system 1;
FIG. 14 shows the construction of a content-log analyzing system 2;
FIG. 15 is a block diagram showing the construction of a data-communication controlling device 40a;
FIG. 16 is a flowchart showing the operation of the content-log analyzing system 2, to be continued to FIG. 17;
FIG. 17 is a flowchart showing the operation of the content-log analyzing system 2, to be continued to FIG. 18; and
FIG. 18 is a flowchart showing the operation of the content-log analyzing system 2.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[First Embodiment]

[0034] The following describes a content-log analyzing system 1 as a first embodiment of the present invention, with reference to the drawings.

<Construction>

[0035] FIG. 1 shows the construction of the content-log analyzing system 1. As shown in the figure, the content-log analyzing system 1 is composed of a broadcast receiving device 10, a TV (television) 20, a PC (personal computer) 30, a data-communication controlling device 40, a content-log analyzing server 50, and a broadcast device 60.

[0036] In FIG. 1, the broadcast receiving device 10, the TV 20, the PC 30, and the data-communication controlling device 40 encircled by a broken line are devices placed in a home of the user who views and/or listens to content. The broadcast receiving device 10, the TV 20, and the PC 30 are each connected to the data-communication controlling device 40 via a LAN cable, and communicate with the data-communication controlling device 40. The content-log analyzing server 50 and the broadcast device 60 are placed in a convent provision center that provides content. The content-log analyzing server 50 is connected to the data-communication controlling device 40 via an Internet 70. The broadcast device 60 broadcasts content via a broadcast satellite 80.

[0037] The following describes each component of the system 1 in detail.

1. Broadcast Receiving Device 10

[0038] The broadcast receiving device 10 receives and stores encrypted content that is broadcasted from the broadcast device 60 via the broadcast satellite 80. Within the home network, the broadcast receiving device 10 is connected to the data-communication controlling device 40 via a LAN cable. The broadcast receiving device 10 receives a request for playing back content (hereafter, a "content request") from the TV 20 or the PC 30 via the data-communication controlling device 40, and transmits the requested content that is in an encrypted form, to the data-communication controlling device 40.

[0039] FIG. 2 is a block diagram showing the construction of the broadcast receiving device 10. As shown in the figure, the broadcast receiving device 10 is composed of a receiving unit 101, a processing unit 102, a content storing unit 103, a controlling unit 104, a communicating unit 105, and a memory unit 106.

(1) Receiving Unit 101

[0040] The receiving unit 101 includes an antenna, and receives, via the antenna, a digital broadcast wave that is broadcasted from the broadcast device 60 via the broadcast satellite 80. The receiving unit 101 extracts, from the received digital broadcast wave, packets that constitute encrypted content, and outputs the extracted packets one after another to the processing unit 102.

(2) Processing Unit 102

[0041] The processing unit 102 receives packets one after another from the receiving unit 101, and reconstructs encrypted content using the received packets, and stores the encrypted content into the content storing unit 103.

(3) Content Storing Unit 103

[0042] The content storing unit 103 is specifically a hard disk unit, and stores encrypted content that is outputted from the processing unit 102.

[0043] The encrypted content 150 shown in FIG. 3 is one example of encrypted content stored in the content storing unit 103.

[0044] As shown in the figure, the encrypted content 150 is composed of header information, encrypted content information, and end code. The header information includes "content ID" 151, "license information" 152, "additional information" 154, "data size of header information", and the like.

[0045] The "content ID" is an ID used to uniquely identify content. The "content ID" 151 of the encrypted content 150 is "Program. 01".

[0046] The "license information" is information describing a content type and copy control information of content. To be specific, the content type is "High-Value" or "Free", and the copy control information is "Copy Free", "Copy Once", "Copy No More", or "Copy Never". In the case of the "license information" 152 of the encrypted content 150, the content type is "High-Value" and the copy control information is "Copy Never".

[0047] The "additional information" is used to judge whether or not to record the communication in the "log" for content's communication (hereafter, the "content-log") when the content is distributed to a certain device within the home network via a LAN cable. The "additional information" is a flag set at "0" or "1" . The additional information being "1" indicates to record the communication in the content-log, whereas the additional information being "2" indicates not to record the communication in the content-log. The "additional information" 154 of the encrypted content 150 is "1". The additional information is described in more detail later.

[0048] The "data size of header information" is a data length of the header information expressed in units of bytes. It should be noted here that the "data size of header information" is not shown in FIG. 3.

[0049] The encrypted content information is specifically main data of the content that has been encrypted by the broadcast device 60 using a content key "KC" as an encryption key, according to the encryption algorithm "E1" To be specific, the DES (Data Encryption Standard) is employed as the encryption algorithm "E1"

[0050] The end code is a predetermined bit sequence representing the end of the content.

(4) Controlling Unit 104

[0051] The controlling unit 104 includes a CPU, a ROM, a RAM, and the like. The controlling unit 104 controls the entire broadcast receiving device 10 by its CPU executing a computer program stored in its ROM.

[0052] The controlling unit 104 receives a content request from the data-communication controlling device 40 via the communicating unit 105. The controlling unit 104 reads a content ID included in the received request, and reads encrypted content having the same content ID, from the content storing unit 103. The controlling unit 104 outputs the read encrypted content to the communicating unit 105.

(5) Communicating Unit 105

[0053] The communicating unit 105 is a LAN-connected unit including an IEEE1394 connector and the like, and is connected to the data-communication controlling device 40 via a LAN cable. The communicating unit 105 receives the encrypted content from the controlling unit 104, divides the encrypted content into packets, and transmits the packets one after another to the data-communication controlling device 40.

(6) Memory Unit 106

[0054] The memory unit 106 is connected to the communicating unit 105. In the memory unit 106, a network address "IPC", a device ID "IDC", and a certificate "CIDC" are stored. The network address "IPC" is an IP address that is transmitted from the data-communication controlling device 40 when the broadcast receiving device 10 is newly connected to the data-communication controlling device 40. The device ID "IDC" is specifically a MAC address assigned to a NIC (Network Interface Card) at the time of manufacture. The certificate "CIDC" has been issued by a certification authority and is used to authenticate the device ID "IDC".

[0055] It should be noted here that the device ID "IDC" and the certificate "CIDC" are stored at an OS level or a BIOS level to prevent them from being tampered by the user.

2. TV 20

[0056] The TV 20 is a device for decoding, and playing

back content, i.e., displaying content. The TV 20 is specifically a computer system that is composed of a microprocessor, a ROM, a RAM, a LAN-connected unit, and the like.

[0057] FIG. 4 is a block diagram showing the construction of the TV 20. As shown in the figure, the TV 20 is composed of a communicating unit 201, a memory unit 202, an input unit 203, a controlling unit 204, a decrypting unit 205, an audio decoder 206, a video decoder 207, a speaker 208, and a monitor 209.

(1) Communicating Unit 201

[0058] The communicating unit 201 is a LAN-connected unit including an IEEE1394 connector and the like. Via a LAN cable, the communicating unit 201 is connected to the data-communication controlling device 40.

[0059] The communicating unit 201 receives a content request, and a network address "IPA" outputted from the controlling unit 204, and transmits the received content request and network address "IPA" to the data-communication controlling device 40.

[0060] Also, the communicating unit 201 receives packets of encrypted content from the data-communication controlling device 40, and outputs the packets of encrypted content to the encrypting unit 205.

(2) Memory Unit 202

[0061] The memory unit 202 is connected to the communicating unit 201. In the memory unit 202, a network address "IPA", a device ID "IDA", and a certificate "CIDA" are stored. The network address "IPA" is an IP address transmitted from the data-communication controlling device 40 when the TV 20 is newly connected to the data-communication controlling device 40. The device ID "IDA" is specifically a MAC address assigned to a NIC at the time of manufacture. The certificate "CIDA" has been issued by a certification authority and is used to authenticate the device ID "IDA".

[0062] It should be noted here that the device ID "IDA" and the certificate "CIDA" are stored at an OS level or a BIOS level to prevent them from being tampered by the user.

(3) Input Unit 203

[0063] The input unit 203 is specifically a user interface including a button and the like. Upon receipt of a user operation of the button and the like, the input unit 203 generates an input signal corresponding to the operation, and outputs the generated input signal to the controlling unit 204.

[0064] When the user operation indicates a request for playing back content, the input unit 203 generates, as the input signal, a content request including a content ID, and outputs the generated content request to the controlling unit 204.

(4) Controlling Unit 204

[0065] The controlling unit 204 includes a CPU, a ROM, a RAM, and the like. The controlling unit 204 controls the entire TV 20 by its CPU executing a computer program stored in its ROM.

[0066] The controlling unit 204 receives an input signal from the input unit 203, and executes processing suitable for the received input signal. Upon receipt of a content request including a content ID as an input signal from the input unit 203, the controlling unit 204 reads the network address "IPA" stored in the memory unit 202, and transmits the read network address "IPA" and the content request, to the data-communication controlling device 40 via the communicating unit 201.

(5) Decrypting Unit 205

[0067] The decrypting unit 205 includes a CPU, a ROM, a RAM, and the like, and internally stores a device key "KA".

[0068] The decrypting unit 205 receives encrypted content from the communicating unit 201, and decrypts the encrypted content in the following way, so as to generate content.

[0069] The decrypting unit 205 first refers to the "data size of header information" included in header information of the encrypted content, to detect a start position of the encrypted content information. The decrypting unit 205 then starts decrypting, from the detected start position, the encrypted content information using the device key "KA" according to the decryption algorithm "D2", so as to generate content information. The decrypting unit 205 continues the decryption process of the encrypted content information until detecting the end code. It should be noted here that an algorithm designed to decrypt data that has been encrypted according to the encryption algorithm "E2" is employed as the decryption algorithm "D2".

[0070] The decrypting unit 205 demultiplexes the content information into an audio stream and a video stream, and outputs the audio stream to the audio decoder 206 and the video stream to the video decoder 207.

(6) Audio Decoder 206

[0071] The audio decoder 206 receives an audio stream from the decrypting unit 205, expands the received audio stream to an audio signal, and outputs the audio signal to the speaker 208.

(7) Video Decoder 207

[0072] The video decoder 207 receives a video stream from the decrypting unit 205, expands the received video stream to a video signal, and outputs the video signal to the monitor 209.

3. PC 30

[0073] The PC 30 is a personal computer system that is composed of a microprocessor, a ROM, a RAM, a hard disk unit, a display unit, a keyboard, a mouse, a LAN-connected unit, and the like.

[0074] FIG. 5 is a block diagram showing the construction of the PC 30. As shown in the figure, the PC 30 is composed of a communicating unit 301, a memory unit 302, an input unit 303, a controlling unit 304, an audio decoder 305, a video decoder 306, a speaker 307, and a monitor 308.

(1) Communicating Unit 301

[0075] The communicating unit 301 is a LAN-connected unit including an IEEE1394 connector and the like, and is connected to the data-communication controlling device 40 via a LAN cable.

[0076] The communicating unit 301 receives a content request and a network address "IPB" from the controlling unit 304, and transmits the received content request and network address to the data-communication controlling device 40.

[0077] Also, the communicating unit 301 receives packets of encrypted content from the data-communication controlling device 40, and outputs the packets of encrypted content to the controlling unit 304.

(2) Memory Unit 302

[0078] The memory unit 302 is connected to the communicating unit 301. In the memory unit 302, a network address "IPB", a device ID "IDB", and a certificate "CIDB" are stored. The network address "IDB" is an IP address transmitted from the data-communication controlling device 40 when the PC 20 is newly connected to the data-communication controlling device 40 as described above. The device ID "IDB" is specifically a MAC address assigned to a NIC at the time of manufacture. The certificate "CIDB" has been issued by a certification authority and is used to authenticate the device ID "IDB".

[0079] It should be noted here that the device ID "IDB" and the certificate "CIDB" are stored at an OS level or a BIOS level to prevent them from being tampered by the user.

(3) Input Unit 303

[0080] The input unit 303 is specifically a user interface including a keyboard, a mouse, and the like. Upon receipt of a user operation of the keyboard, mouse, or the like, the input unit 303 generates an input signal corresponding to the operation, and outputs the generated input signal to the controlling unit 304.

[0081] When the user operation indicates a request for playing back content, the input unit 303 generates, as the input signal, a content request including a content ID, and outputs the generated content request to the controlling unit 304.

(4) Controlling Unit 304

[0082] The controlling unit 304 includes a CPU, a ROM, a RAM, an HDD, and the like. The controlling unit 304 controls the entire PC 30 by its CPU executing a computer program stored in its ROM or HDD.

[0083] The controlling unit 304 receives an input signal from the input unit 303, and executes processing suitable for the received input signal. Upon receipt of a content request including a content ID as an input signal from the input unit 303, the controlling unit 304 reads the network address "IPB" stored in the memory unit 302, and transmits the read network address "IPB" and the content request, to the data-communication controlling device 40 via the communicating unit 301.

[0084] Also, the controlling unit 304 internally stores a device key "KB". The device key "KB" is a decryption key to be used to decrypt encrypted content when the PC 30 receives the encrypted content from the data-communication controlling device 40.

[0085] Upon receipt of encrypted content including encrypted content information encrypted using the device key "KB" from the data-communication controlling device 40, the controlling unit 304 decrypts the encrypted content in the following way, so as to generate content.

[0086] The controlling unit 304 first refers to the "data size of header information" included in header information of the encrypted content, to detect a start position of the encrypted content information. The controlling unit 304 then starts decrypting, from the detected start position, the encrypted content information using the device key "KB" as a decryption key, according to the decryption algorithm "D2", so as to generate content information. The controlling unit 304 continues the decryption process of the encrypted content information until detecting the end code. The controlling unit 304 demultiplexes the content information, into an audio stream and a video stream, and outputs the audio stream to the audio decoder 305 and the video stream to the video decoder 306.

(5) Audio Decoder 305

[0087] The audio decoder 305 receives an audio stream from the controlling unit 304, expands the received audio stream to an audio signal, and outputs the audio signal to the speaker 307.

(6) Video Decoder 306

[0088] The video decoder 306 receives a video stream from the controlling unit 304, expands the received video stream to a video signal, and outputs the video signal to the monitor 308.